Collège du Cèdre au Vésinet 2018-2019

EPI Français-mathématiques

6ème

Sur les traces d'Arsène Lupin

Conception du jeu en 6ème

Ce jeu a été réalisé grâce à la collaboration de nombreuses personnes :
Les élèves d'une classe de 6ème du collège du Cèdre au Vésinet, un professeur de mathématiques et un professeur de français.
L'idée a été de jouer avec les codes secrets en les découvrant à travers un livre :
L'aiguille creuse de Maurice Leblanc.
Le jeu a ensuite été conçu en rapport avec le livre : au fil du jeu, d'une énigme à l'autre, d'un code à l'autre, on peut suivre le cours de l'histoire de Maurice Leblanc.
Nous avons choisi de nous inspirer d'un jeu existant : « Les mystères de Pékin ».

Utilisation des mathématiques en 6ème

Dans ce jeu, les mathématiques sont utilisées à de multiples occasions :
- Tout d'abord pour concevoir le jeu : il a fallu réfléchir à la notion de code secret, comment en créer, et se demander à chaque fois : est-il possible de déchiffrer le message facilement. Les élèves ont ainsi fait un voyage dans le temps et ont découvert et calculé des fréquences.
- Ensuite pour fabriquer le jeu :
Pour créer les codes secrets, les élèves ont caché des messages à l'aide de geogebra. Ils l'ont repéré à l'aide d'angles. Ils ont aussi calculé des mesures d'angles pour créer sur geogebra le fameux code César : ils ont obtenu un fichier permettant de faire tourner le disque virtuellement, et l'ont aussi décoré à la main.
Les élèves se sont repérés dans le carré de Polybe.
Puis pour rendre plus compliqué les codes, ils ont voulu se passer d'un ordre alphabétique et ont fait beaucoup d'opérations avec le chiffrage affine ; enfin voulant vaincre la méthode des fréquences, ils se sont repérés dans le carré de Vigenère.
Pour fabriquer le jeu certains ont fait des prouesses en dessin et en peinture : ils ont fabriqué plateau et accessoires. Ils ont fabriqué leurs dés, en essayant qu'ils soient bien équilibrés. Ils ont aussi utilisé des patrons de pavé pour fabriquer leurs pions, et même une boîte à pions.
- Enfin pour utiliser le jeu :
Les joueurs doivent utiliser les accessoires, réfléchir, faire quelques opérations, mesurer des angles.

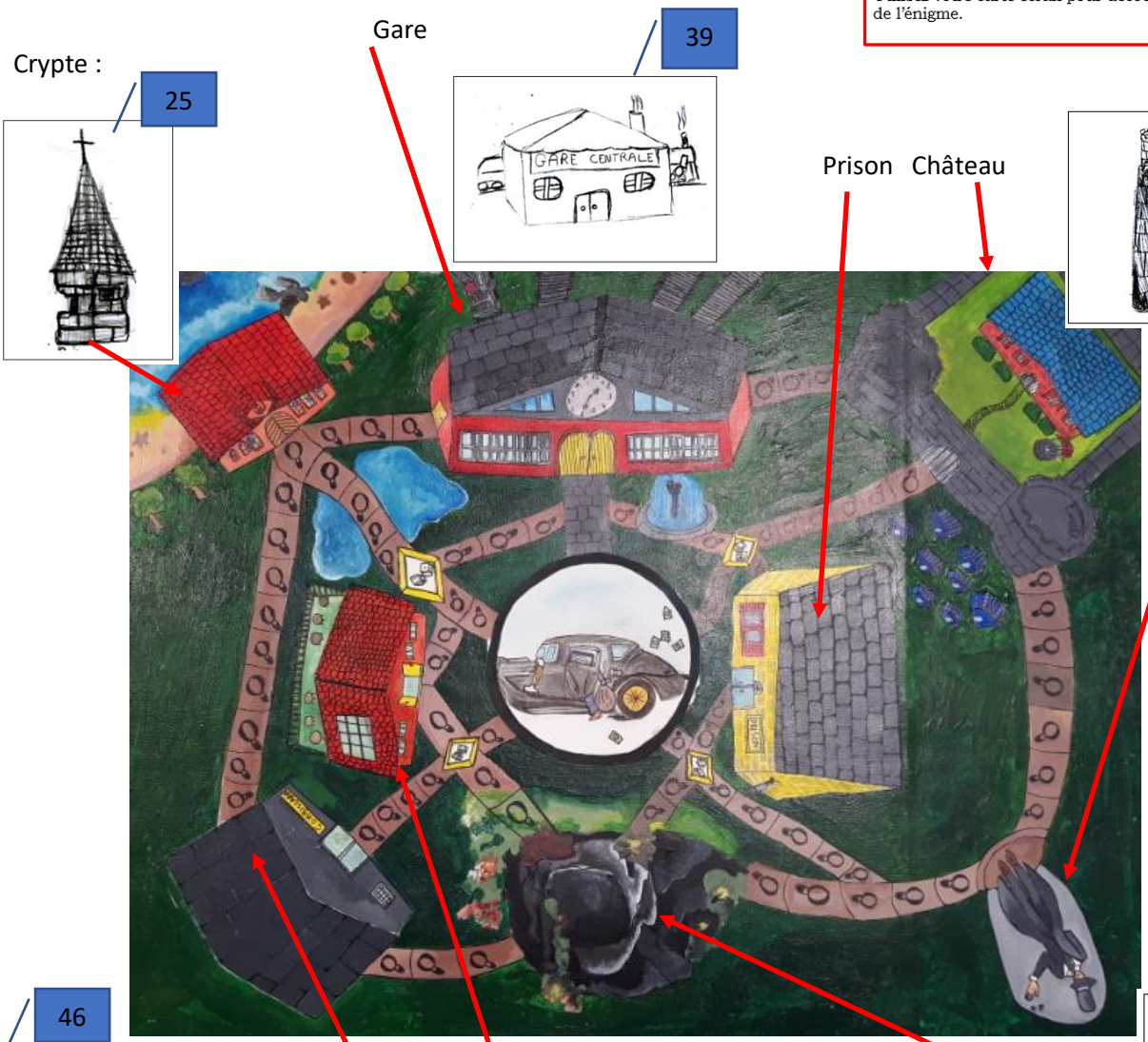
Règle du jeu, énigmes

En français, les élèves ont écrit la règle du jeu et un livret de huit énigmes, à la manière du vrai jeu, « Les Mystères de Pékin ». La règle du jeu est très proche de la véritable règle. Les énigmes sont toutes en rapport avec le livre de Maurice Leblanc. Les élèves ont dessiné, colorié, numéroté les cartes, certains ont peint le plateau.

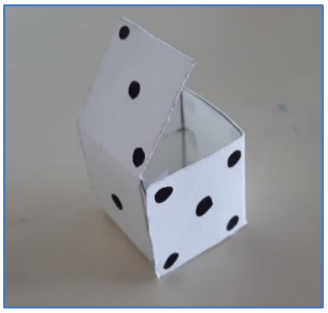
Exemple de partie : avec l'énigme n°2

Dans cette énigme, le personnage de Maurice Leblanc, Jean Daval, a été tué. Il s'agit de découvrir qui est le meurtrier, pourquoi et comment.

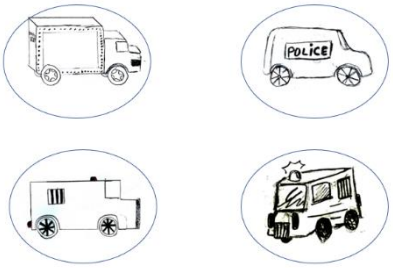
Les joueurs placent les cartes numérotées indiquées à l'endroit approprié du plateau (il y a une case gare, une case château…).



Les joueurs placent leurs pions au centre, prennent le dé fabriqué :

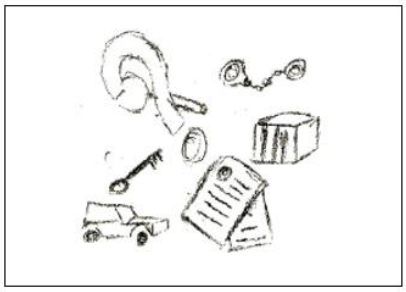


Ils placent quatre fourgons (les dragons dans le vrai jeu) :



Enfin les joueurs placent un paquet de cartes chances (fabriquées par les élèves) sur le plateau et prennent leur feuille de recherches.

Exemple de « carte chance »



La partie se déroule suivant les règles indiquées dans le livret écrit par les élèves en cours de français.

Conception du jeu, exemple avec l'énigme 2 :

- un joueur tombe sur l'un des lieux : château, crypte, commissariat : dans ce cas, le jeu est fait de sorte que une fois décrypté, le joueur gagne un indice décisif.

Par exemple dans l'énigme 2, on obtient à la fin les trois réponses attendues dans l'énigme, qui sont :

- « C'est le comte de Gesvres qui a tué Jean Daval. »
- « C'était de la légitime défense. »
- « Le meurtrier a utilisé un couteau. »

- un joueur tombe sur l'un des lieux : café, gare, grotte, il pourra lire : « il n'y a pas d'indice »
- un joueur tombe sur Arsène Lupin : il trouvera un indice : « Rendez-vous au commissariat et au château. »

Le joueur pensant avoir découvert en premier la solution de l'énigme vérifie à l'aide de la carte écran rouge et du livret d'énigme.

Cartes de l'énigme 2 :
D'un côté on a ceci :

Et de l'autre :

Les cartes sont numérotées pour 8 énigmes, certaines en double sont retirées.
Pour le joueur une carte quel code choisir est donnée (pour que la partie ne soit pas trop longue…) :

Voici donc les accessoires à utiliser ainsi qu'une aide précieuse :

- pour le code « Vigenère », les mots secrets font partie de la liste suivante: sixième, Hector, ArseneLupin ou Etretat
- pour le code César, le décalage sera de : 2 ou 3 ou 17
- pour le codage affine, il y aura deux possibilités correspondant aux calculs : y = 3x+2 ou y =5x+1
- pour la scytale, il y a un choix entre trois modèles.

Pour l'énigme 2

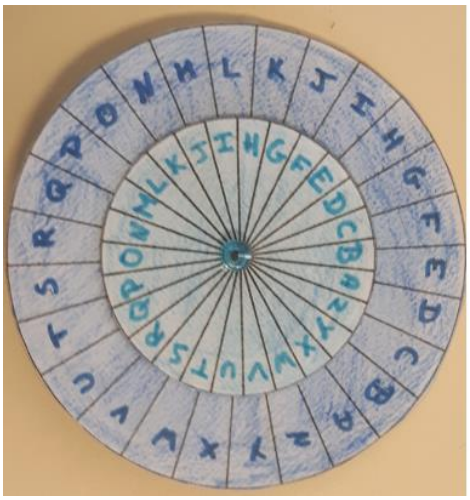
Carte à coder	Numéro	Code ou fichier
Arsène Lupin	34	Code César
Café	78	Morse
Château	63	Vigenère
Commissariat	46	Morse
Crypte	25	Polybe
Gare	39	Geogebra
Grotte	54	Affine

Les réponses de l'énigme 2 :

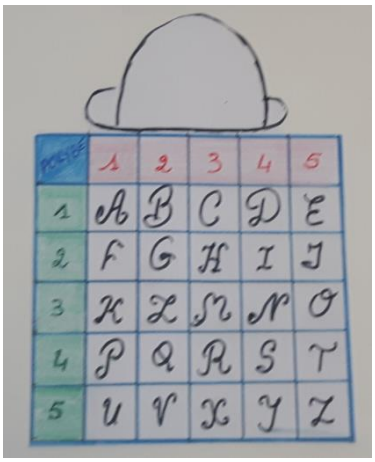
Arsène Lupin	34	Rendez-vous au commissariat et au château
Café	78	Il n'y a aucun indice ici
Château	63	C'est le comte de Gesvres qui a tué Jean Daval.
Commissariat	46	C'était de la légitime défense.
Crypte	25	Le meurtrier a utilisé un couteau.
Gare	39	Il n'y a aucun indice ici
Grotte	54	Il n'y a aucun indice ici

Pour décrypter, voici les accessoires créés par les 6èmes pour les 7 méthodes vues

Code César (1 en papier, 1 sous geogebra)

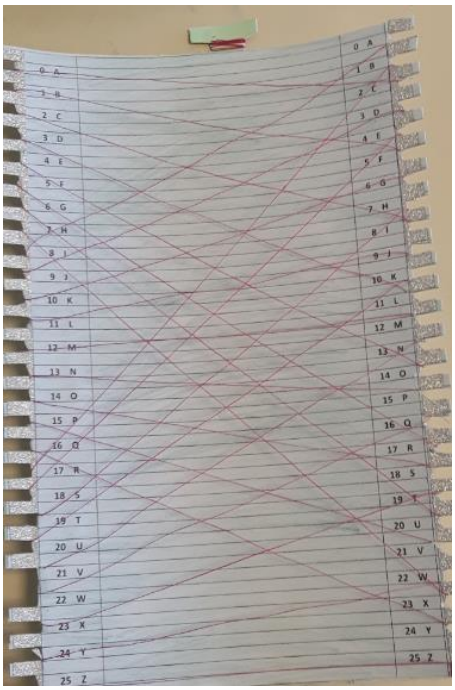


Carré de Polybe

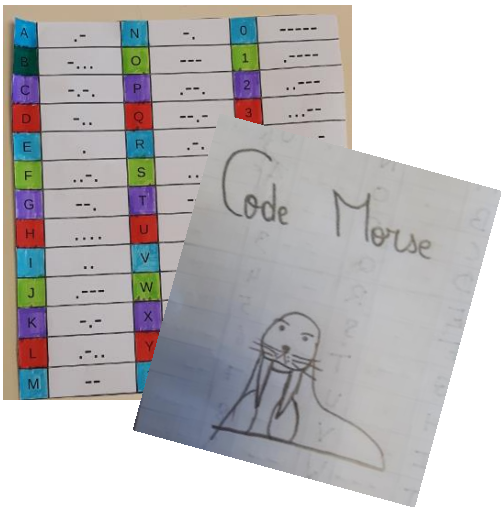


Scytales (choix entre 3 scytales)

Chiffrage affine (2 choix proposés)

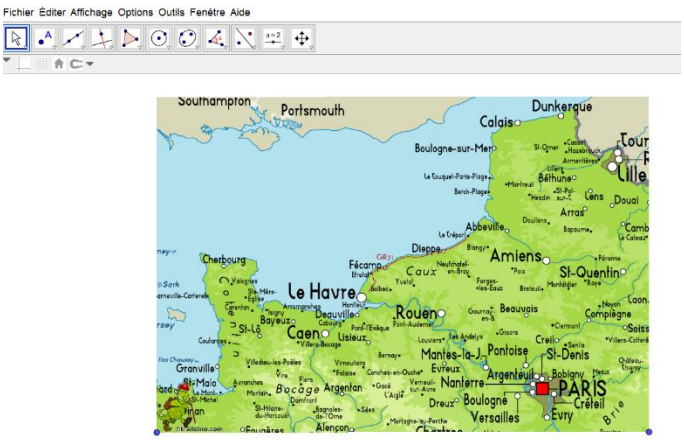


Code Morse



Vigenère

Stéganographie (1 fichier par énigme, message caché)



Voici maintenant les travaux effectués en cours de mathématiques pour comprendre et savoir crypter et décryptés les messages écrits sur les cartes.

Les codes secrets

Fiche 1 Vocabulaire

Rechercher les définitions des mots suivants :

1) Cryptologie
2) Cryptographie
3) Cryptanalyse

Fiche 1 correction

Lexique du magazine « Les cahiers de sciences et vie » n°133

Cryptologie : sciences des messages secrets. Elle se divise en deux grandes branches : la cryptographie et la cryptanalyse.

Cryptographie : art de transformer un message clair en un message inintelligible pour celui qui ne possède pas les clés de chiffrement.

Cryptanalyse : art d'analyser un message chiffré afin de le décrypter.

Complément :

Chiffrement : procédé de transformation des données d'un document à l'aide d'un algorithme, permettant de les rendre inintelligibles à toute personne ne disposant pas de clé d'encodage.

Déchiffrement : Opération inverse du chiffrement, permettant de revenir à la version en clair d'un message chiffré en connaissant la méthode de chiffrement et les clés.

Clé : Nombre, mot, phrase, … qui permet, grâce à l'algorithme, de chiffrer un message.

Voici quelques procédés que nous détaillerons :

- Stéganographie
- Substitution
- Transposition

Fiche 2 Stéganographie : exemple avec geogebra

Stéganographie : procédé qui consiste non pas à rendre le message inintelligible, mais à le camoufler dans un support de manière à masquer son existence.

I Cacher le message

1. Ouvrir un fichier sur geogebra
2. Repérer un support pour cacher le message : par exemple une carte. Une carte a été mise dans vos documents. Avec « Fichier », puis « ouvrir » choisir « carte ». L'ouvrir puis avec le bouton droit de la souris, « copier » l'image.
   Insérer cette carte sur geogebra : pour cela, il suffit de repérer vers le haut le menu « éditer » puis « insérer Image depuis presse-papier ».
   Deux points apparaissent en bas de l'image. Afficher leurs « étiquettes » : celui de gauche s'appelle A et celui de droite s'appelle B.
   On peut déplacer et agrandir l'image à l'aide de ces deux points.
3. Il faut ensuite créer le message secret : par exemple on peut prendre une photo du message à cacher et l'insérer lui aussi dans geogebra : la photo d'un trésor se trouve dans vos documents. Ouvrez le fichier « Image coffre », copiez-le et insérer-le dans geogebra. Laisser le trésor à côté de la carte, le temps de trouver une cachette.

4. Repérer ensuite un endroit précis où on veut insérer le message, ici, le coffre. Marquer un point E à côté. Nous mettrons le trésor à côté à la fin et nous enlèverons toute trace de notre passage (E).

II Trouver le message (destinataire)

1. Il faudra donc laisser un indice pour retrouver le trésor, donc le point E : pour cela, on peut par exemple tracer les trois côtés du triangle ABE. Le côté [AB] étant en fait le bas de la photo, on peut repérer le point E à l'aide de deux **angles** :

- A gauche l'angle de sommet A et de côtés [AB] et [AE]. Il se nomme : $\widehat{BAE}$ (ou $\widehat{EAB}$).
- A droite l'angle de sommet ……. et de côtés ……. et ……. . Il se nomme : …….
  Chacun de ces angles se mesure dans une unité : le **degré** noté ..°.
  Un angle se mesure à l'aide d'un **rapporteur.**
  Geogebra sait les mesurer : pour cela, repérer l'instruction **« angle ».**
- Pour mesurer l'angle de gauche, il faut cliquer sur B, puis le sommet de l'angle A, et enfin sur E.
  Un nombre s'affiche : c'est la mesure de l'angle $\widehat{BAE}$.
- Faire de même pour l'angle de droite, mais en commençant par E, puis le sommet de l'angle B, et enfin A.
- Revenir sur la flèche du « déplacer » en haut à gauche, puis observer les mesures des deux angles quand vous déplacez le point C sur la carte. Quand vous êtes sûr de la place du coffre, noter ci-dessous les deux angles, vous pouvez arrondir à l'unité.
  En A : …….. en B : ……
  La mesure de ces deux angles change-t-elle en zoomant ou dézoomant sur la carte ? ……

2. Déplacer le trésor avec les deux points au bas de l'image coffre, les placer à l'endroit voulu, très proches l'un de l'autre, à proximité de E. Masquer tous les autres points et traits. Quand vous ne distinguez plus le coffre, ou presque plus, vous pouvez masquer les deux derniers points.

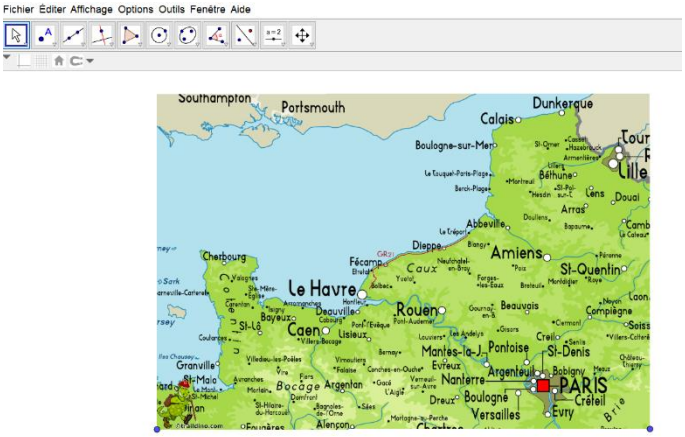
   Le trésor est caché.

3. Quels indices donner à un enquêteur pour qu'il le retrouve, sans lui donner le droit de regarder dans les propriétés ni revenir en arrière ?

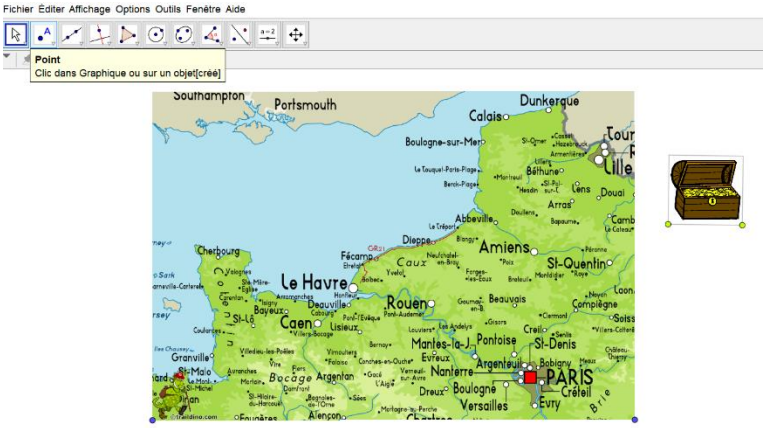
……
……

Fiche2 Stéganographie : correction

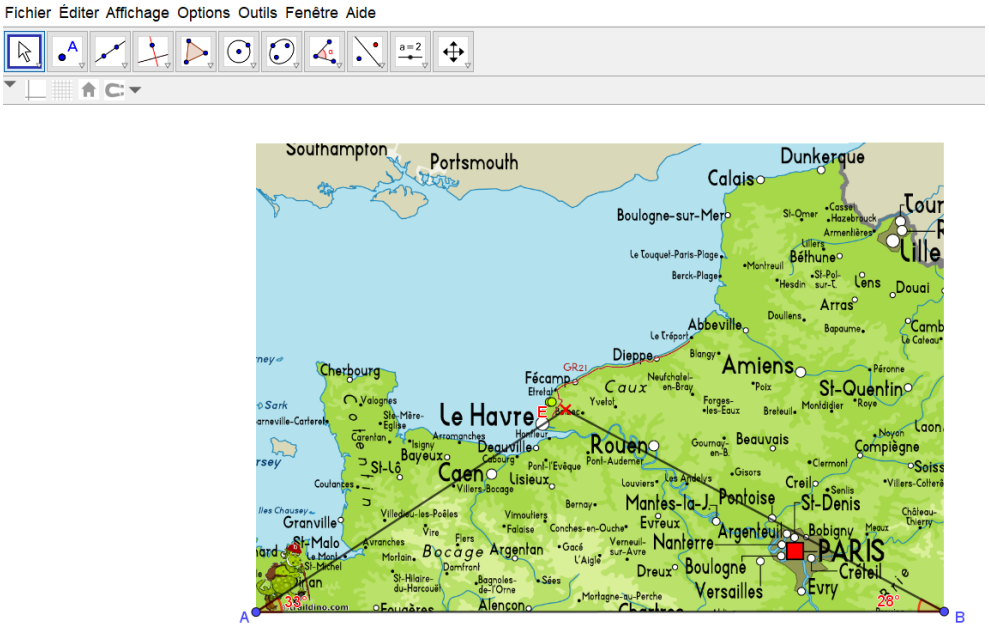
Etape 1



Etape 2



Etape 3



Etape 4 :

Il faut que l'enquêteur trouve les angles, repère ensuite l'endroit, et **zoome…**

Fiche 2 (suite) Stéganographie

1. La stéganographie dans l'histoire

Le Grec Hérodote(-480 ;– 425 environ), historien, a raconté les guerres entre les Grecs et les Perses, et en particulier : deux méthodes de stéganographie.

Première méthode :

Histiée était le tyran de la cité grecque de Milet, sous domination perse. Nommé conseiller à la cour du roi de Perse, il a cédé le pouvoir à Aristagoras. Pour des raisons assez complexes, il a décidé d'encourager Aristagoras à prendre la tête d'un mouvement de révolte contre les Perses.
Ainsi, Histiée voulut communiquer avec Aristagoras pour l'inciter à se révolter. Comme les routes étaient surveillées, il ne pouvait procéder de manière ordinaire. Il rasa donc la tête de son plus fidèle serviteur, y inscrivit son message, puis attendit que les cheveux repoussent. Dès qu'ils furent assez longs, il l'envoya à Milet en lui donnant simplement les instructions suivantes : une fois qu'il serait arrivé à Milet, il devrait demander à Aristagoras de lui couper les cheveux, puis de regarder ce qu'il avait sur la tête. Le message incitait Aristagoras à se révolter.

Deuxième méthode

Un autre passage raconte l'histoire de Demarate, ancien roi de Sparte réfugié auprès du roi des Perses, Xerxès Ier, qui a succédé à Darius. Demarate fut mis au courant d'un projet d'invasion de la Grèce. Il décida alors de prévenir Sparte en toute discrétion en utilisant le stratagème suivant :
"Il prit une tablette double, en gratta la cire, puis écrivit sur le bois même les projets de Xerxès; ensuite il recouvrit de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis."
Les tablettes étant arrivées à Sparte, la cire fut grattée et on découvrit ainsi le message de Démarate.

Source historique : http://mercure.fltr.ucl.ac.be/Hodoi/concordances/herodote_historiae_05/lecture/4.htm
Hérodote, Histoires, livre V Chapitres 30-39 [5,35] XXXV.

2. L'encre invisible

Un moyen stéganographique qui a traversé les siècles est celui de l'encre invisible. Elle provient de matériaux d'origine organique, comme le jus de citron, la sève de plantes, en raison de leur haute teneur naturelle en carbone, et donc de leur tendance à noircir lorsqu'ils sont soumis à des températures peu élevées, comme la flamme d'une bougie.

3. La stéganographie numérique

Grâce à l'informatique, les images peuvent être traitées. Il est facile de les modifier en taille, en couleur, d'ajouter ou supprimer tel ou tel élément, d'appliquer des filtres variés, etc.

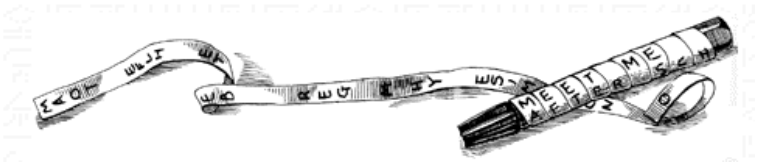
Fiche 3 Transposition : scytale

Transposition : un chiffre de transposition conserve l'identité des caractères du texte clair mais change leur ordre (permutation).

Source : livre « Les codes secrets décryptés » de Didier Müller :

En 404 avant J.-C., Lysandre de Sparte vit arriver un messager ensanglanté, l'un des cinq survivants d'un éprouvant voyage depuis la Perse. Le messager tendit sa ceinture à Lysandre qui l'entoura autour de sa scytale et apprit que Phranabaze de Perse s'apprêtait à l'attaquer. Grâce à la scytale, Lysandre se prépara à cette attaque et le repoussa.

***Référence historique : PLUTARQUE** / Vies des hommes illustres*
« Voici, du reste, ce que c'est que la scytale. Quand un général part pour une expédition de terre ou de mer, les éphores prennent deux bâtons ronds, parfaitement égaux en longueur et en grosseur, de façon à se correspondre exactement l'un à l'autre, dans toutes les dimensions. Ils gardent l'un de ces bâtons, et donnent l'autre au général: ils appellent ces bâtons scytales. Lorsqu'ils veulent mander au général quelque secret d'importance, ils taillent une bande de parchemin, longue et étroite comme une courroie, la roule autour de la scytale qu'ils ont gardée, sans laisser le moindre intervalle entre les bords de la bande, de telle sorte que le parchemin couvre entièrement la surface du bâton. Sur ce parchemin ainsi roulé autour de la scytale, ils écrivent ce qu'ils veulent; et, quand ils ont écrit, ils enlèvent la bande, et l'envoient au général sans le bâton. Le général qui l'a reçue n'y saurait rien lire d'ailleurs, parce que les mots, tout dérangés et épars, ne forment aucune suite; mais il prend la scytale qu'il a emportée, et il roule alentour la bande de parchemin, dont les différents tours, se trouvant alors réunis, remettent les mots dans l'ordre dans lequel ils ont été écrits, et présentent toute la suite de la lettre. On appelle cette lettre scytale, du nom même du bâton, comme ce qui est mesuré prend le nom de ce qui lui sert de mesure. »*
** Éphores : Magistrats lacédémoniens (Sparte)*



Ainsi la scytale est le premier dispositif de cryptographie militaire connu : autour d'un bâton de bois était enroulé une bande de cuir ou de parchemin. Une fois écrit, le messager emportait la bande de cuir comme une ceinture, les lettres tournées vers l'intérieur.

Avantage : même en connaissant la technique utilisée, celui qui interceptait le message avait beaucoup de difficulté à le déchiffrer, s'il ne disposait pas des dimensions exactes de la scytale. La longueur et la grosseur de celle-ci étaient finalement la clé du système. Quand la bande était déroulée, le message était illisible par ceux qui ne connaissaient pas la méthode ou qui ne disposaient pas d'un bâton de la même épaisseur.

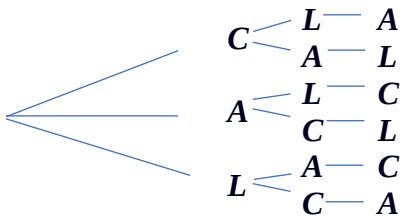
Cette méthode est une méthode de transposition.

Message obtenu : **« Concours MATHS EN JEUX La date limite d'envoi est fixée au vendredi 5 avril 2019 »**

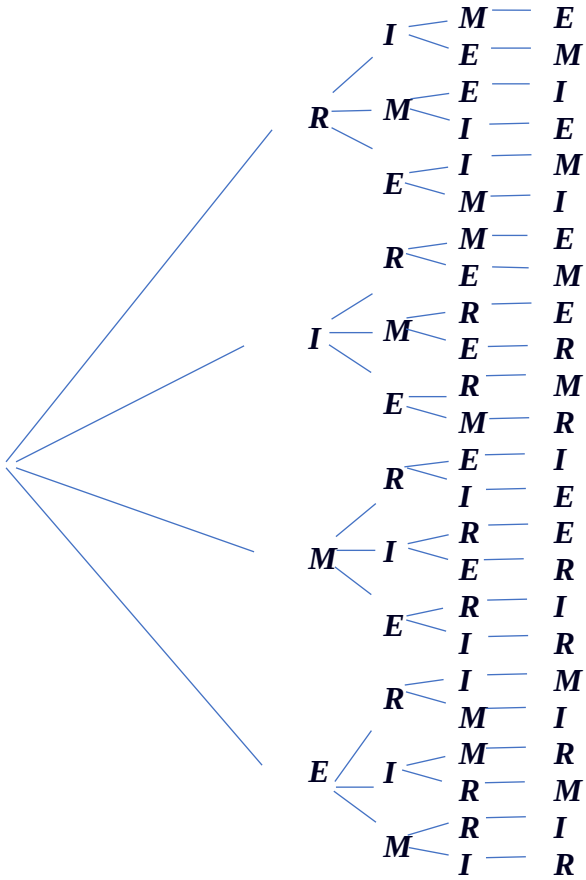
Questions
a) En supposant que le message comprenne 3 lettres, combien y a-t-il de manières de les organiser ? Ecrire toutes les possibilités avec le mot « LAC ».
b) En supposant que le message comprenne 4 lettres, combien y a-t-il de manières de les organiser ? Ecrire toutes les possibilités avec le mot « RIME ».
c) En supposant que le message comprenne 10 lettres, combien y a-t-il de manières de les organiser ? Ecrire toutes les possibilités est-il simple ?
d) Créez votre propre message avec le support de votre choix.
e) Comment s'y prendre pour taper le message à l'aide du traitement de texte de l'ordinateur ? Essayer (si possible) d'obtenir ce qui a été distribué, donc avec 65 lettres, ceci sans tenir compte des espaces ni de la ponctuation. Indication : on peut les présenter dans un tableau.

Fiche 3 Transposition : scytale correction

a) En supposant que le message comprenne 3 lettres, combien y a-t-il de manières de les organiser ?
3 !=3×2×1 = 6
Ecrire toutes les possibilités avec le mot « LAC » :



b) En supposant que le message comprenne 4 lettres, combien y a-t-il de manières de les organiser ?
4 !=4×3×2×1=24
Ecrire toutes les possibilités avec le mot « RIME » :



c) En supposant que le message comprenne 10 lettres, combien y a-t-il de manières de les organiser ?
10 != 10×9×8×7×6×5×4×3×2×1 = 3 628 800

e) Exemple

Voici le message à envoyer :

« Concours MATHS EN JEUX : La date limite d'envoi est fixée au vendredi 5 avril 2019. »

On peut l'écrire directement ou réfléchir au nombre de tour et de lettre par tour.

Il y a **65 lettres** (sans compter espaces et ponctuation).

- Si on veut faire 16 tours (ou si on souhaite surtout 4 lettres par tour):

$65=16\times4+1$

Il faut donc 15 tours avec 4 lettres par tour.

Il y aura un $16^{ème}$ tour avec 5 lettres.

Le plus simple est de l'écrire à la main sur du papier déjà enroulé, puis de le photocopier pour que cela ne se voit pas.

Pour le taper à l'ordinateur : on peut par exemple créer un tableau de 16 colonnes et 5 lignes puis écrire les lettres dedans. Il faut ensuite adapter les caractères à la taille du cylindre choisi : la hauteur de la première colonne doit mesurer autant que le « tour » de l'objet choisi (le problème étant le décalage obtenu en tournant autour).

On imprime puis on découpe colonne par colonne ; enfin on colle les morceaux les uns sous les autres.

C	o	n	c	o	u	r	s	M	A	T	H	S	E	N	J
E	U	X	L	a	d	a	t	e	l	i	m	i	t	e	D'
e	n	v	o	i	e	s	t	f	i	x	é	e	a	u	v
e	n	d	r	e	d	i	5	a	v	r	i	l	2	0	1
9															

Le résultat est :

CEEE9OUNNNXVDCLOROAIEUDEDRASISTT5MEFAALIVTIXRHMEISIELETA2NEU0JD'V1

- Si on veut faire 13 tours (ou si on souhaite 5 lettres par tour):

$65=13\times5$

Il faut donc 13 tours avec 5 lettres par tour.

Pour le taper à l'ordinateur : on peut par exemple créer un tableau de 13 colonnes et 5 lignes puis écrire les lettres dedans.

C	o	n	c	o	u	r	s	M	A	T	H	S
E	N	J	E	U	X	L	a	d	a	t	e	l
i	m	i	t	e	D'	e	n	v	o	i	e	s
t	f	i	x	é	e	a	u	v	e	n	d	r
e	d	i	5	a	v	r	i	l	2	0	1	9

Le résultat est :

CEITEONMFDNJIIICETX5OUEEAUXDEVRLEARSANUIMDVVLAAOE2TTIN0HEED1SLSR9

Pour décrypter, à partir du c, il suffit de compter de 5 en 5.

Remarque : vous pouvez faire des essais à l'aide du site : https://www.dcode.fr/chiffre-scytale

Fiche 4 Substitution

Substitution : un chiffre de substitution remplace les caractères du message en clair par des symboles définis à l'avance.

1. Chiffre de Polybe

Polybe, historien grec (env. 200 - 125 av. J.-C.), est à l'origine du premier procédé de **chiffrement par substitution.** C'est un système de transmission basé sur un carré de 25 cases.
Les lettres sont repérées par une paire de chiffres correspondant à leur rangée et leur colonne.
Avec l'alphabet grec il y avait 24 lettres.
(http://remacle.org/bloodwolf/historiens/polybe/dix.htm)
Il en existe plusieurs versions modernes.
Voici l'une de ces versions (version française avec W au même endroit que V) :

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	j
3	k	l	m	n	o
4	p	q	r	s	t
5	u	v	x	y	z

Ainsi chaque lettre est représentée par un groupe de deux chiffres : en premier la ligne et en deuxième la colonne.
Par exemple la lettre « e » devient : 15.
Le mot « CODE » devient : 13351415.
Pour le déchiffrement on groupe les chiffres 2 par 2, le 1er étant la ligne et le 2ème la colonne.
Par exemple, 413532541215 est en fait : Polybe.

Ce procédé de communication permet la transmission de n'importe quel message en utilisant des signaux, par exemple des torches :

Dans l'antiquité, ce tableau était divisé en 5 tablettes, les 5 colonnes : celui qui envoyait le message montrait des torches à gauche pour indiquer la colonne (donc la tablette), et un autre des torches à droite pour donner la rangée donc la lettre.

Transmission de la lettre "e"

Question : utiliser ce procédé pour déchiffrer un résumé du règlement du concours :

321544 153215521544 14352452153445 4315113224441543 5134 251551 321544 33114523153311 452442511544 44154352153445 32354344 1415 3215321112354311452435343551 325145243224 441145243534 1451 251551 3215 251551 154445 213551433424 14113444 513415 1235244515 1152 1513 3211 343545241315

Réponse :

LES ELEVES DOIVENT REALISER UN JEU LES MATHEMATIQUES SERVENT LORS DE L ELABORATION OU L UTILISATION DU JEU LE JEU EST FOURNI DANS UNE BOITE AVEC LA NOTICE

https://euler.ac-versailles.fr/wm3/pi2/crypto/polybe1.jsp

Fiche 5 Substitution : deuxième exemple

2. Code de César

A la différence de la transposition, la substitution change une lettre pour une autre, en fait par un symbole quelconque. Lors d'une transposition, la lettre change de position mais garde son rôle alors que pour la substitution elle garde sa position mais change de signification.

L'un des premiers algorithmes de substitution était le chiffre de Polybe.

A peu près cinquante année plus tard est apparu un autre chiffrement par substitution, connu sous le nom de code de César. Il chiffrait sa correspondance personnelle au moyen d'un algorithme de substitution de ce type.

On trouve une description du chiffre de César dans les *Vies des douze Césars* de Suétone:

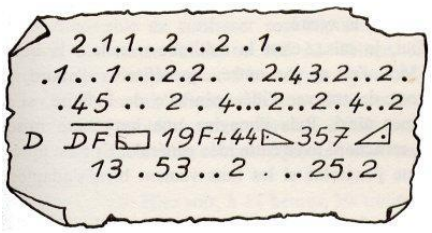
Question : déchiffrer le texte de Suétone :

RQDFRQVHUYHQRXWUHVHVOHWWUHVFLFURQHWFHOOHVTXLODGUHVVDLWVHVIDPLOLHUVVXUV
HVDIIDLUHVGRPHVWLTXHVTXDQGLODYDLWOHXUIDLUHTXHOTXHFRPPXQLFDWLRQVHFUWHLOXVDLW
GXQFKLIIUHFHVWGLUHTXLOEURXLOODLWOHVOHWWUHVGHWHOOHIDRQTXRQQHSWUHFRQVWLW
XHUDXFXQPRWVLORQYHXWHQGFRXYULUOHVHQVHWOHVGFKLIIUHULOIDXWVXEVWLWXHUFKDT
XHOHWWUHODWURLVLPHTXLODVXLWGDQVODOSKDEHWFHVWGLUHOHGODHWDLQVLGHVXLWH

Indications :

- chaque lettre du message original était remplacée par celle qui suivait de …. Positions plus loin dans l'alphabet : la lettre A était remplacée par …, le B par un …, et ainsi de suite.

- pour déchiffrer le message, la technique est décrite dans Arsène Lupin L'aiguille creuse de Maurice Leblanc.



Fiche 5 Substitution : deuxième exemple (suite)

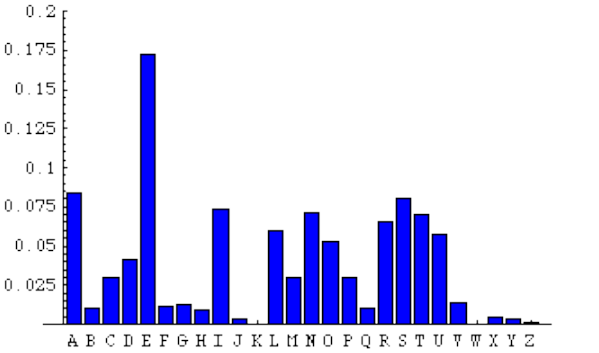
Fréquence des lettres en français :

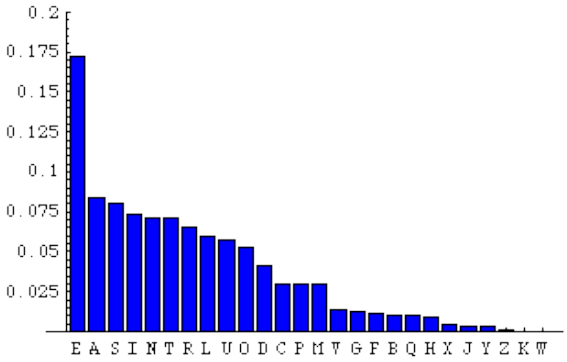
http://www.apprendre-en-ligne.net/crypto/stat/index.html

Ce système a résisté aux cryptanalystes jusqu'à ce que le savant arabe **al-Kindi** mette au point, au IXème siècle, une technique appelée analyse des fréquences.
Al-Kindi (801-873) rédige sa méthode dans son plus important traité intitulé *Manuscrit sur le déchiffrement des messages cryptographiques.* C'est le premier manuscrit connu faisant mention des fréquences d'apparition des lettres
Il explique que « la façon d'élucider un message crypté, si nous savons dans quelle langue il est écrit, est de nous procurer un autre texte en clair dans la même langue, de la longueur d'un feuillet environ, et de compter alors les apparitions de chaque lettre. Ensuite, nous nous reportons au texte chiffré que nous voulons éclaircir et relevons de même ses symboles. Nous remplaçons le symbole le plus fréquent par la lettre première (la plus fréquente du texte clair), le suivant par la deuxième, le suivant par la troisième, et ainsi de suite jusqu'à ce que nous soyons venus à bout de tous les symboles du cryptogramme à résoudre ».

Cette technique ne fonctionne bien que si le cryptogramme est suffisamment long pour avoir des moyennes significatives.

Fréquences d'apparition des lettres			
Lettre	Fréquence	Lettre	Fréquence
A	8.40 %	N	7.13 %
B	1.06 %	O	5.26 %
C	3.03 %	P	3.01 %
D	4.18 %	Q	0.99 %
E	17.26 %	R	6.55 %
F	1.12 %	S	8.08 %
G	1.27 %	T	7.07 %
H	0.92 %	U	5.74 %
I	7.34 %	V	1.32 %
J	0.31 %	W	0.04 %
K	0.05 %	X	0.45 %
L	6.01 %	Y	0.30 %
M	2.96 %	Z	0.12 %

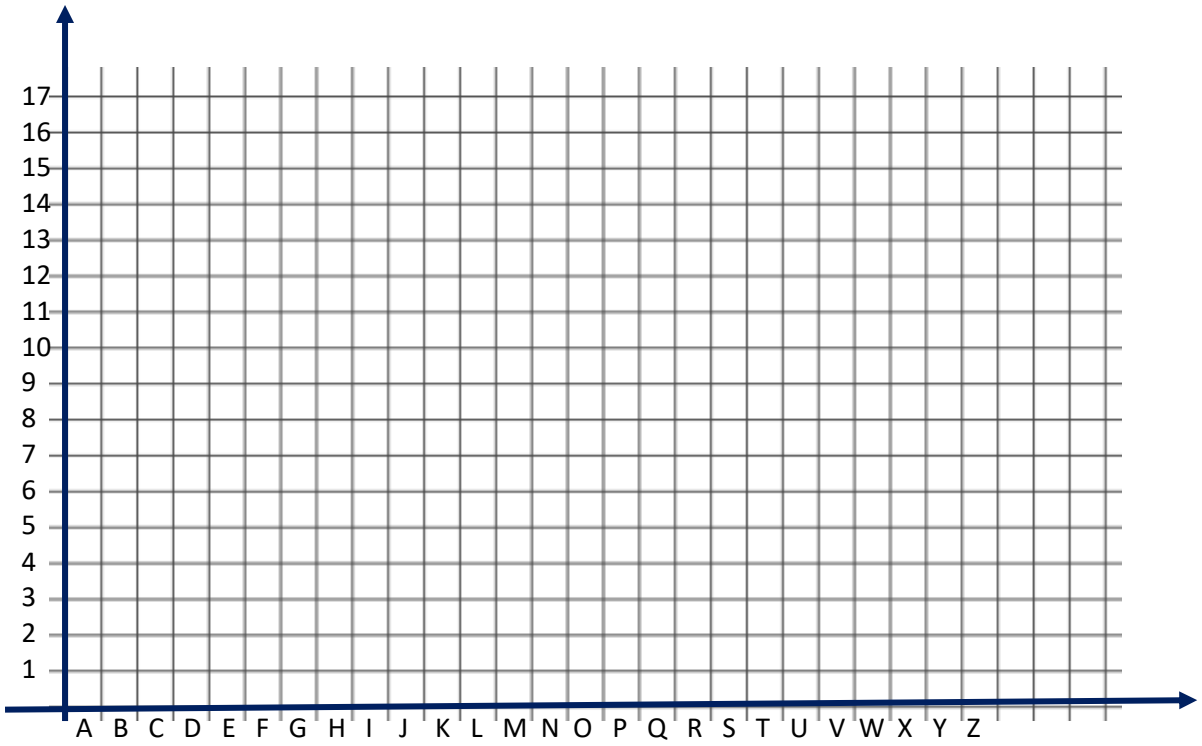




Fiche 5 Substitution : deuxième exemple (fin)

Fréquence des lettres de notre texte : **Dans notre alphabet il y a …. Lettres.**

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Effectif (dans notre texte)																										
Fréquence en %																										



Lettre du texte	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Véritable lettre																										

Question : comment faciliter le déchiffrement ?

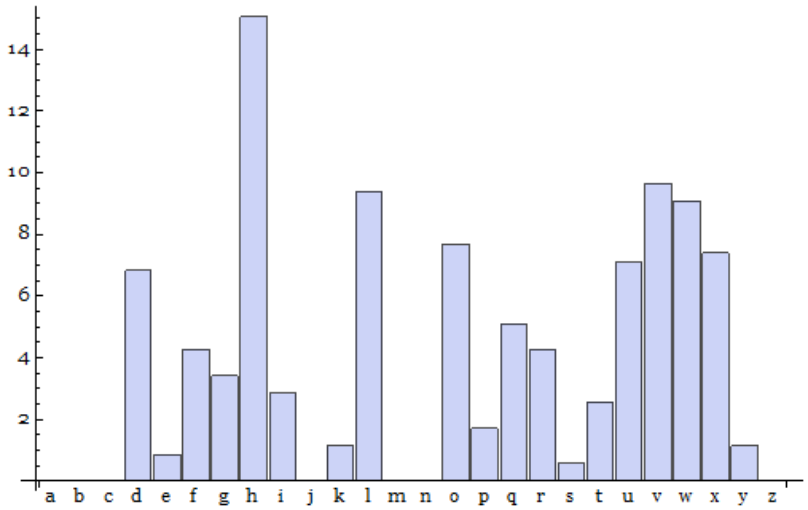
Le texte devient :

Pour un gain de temps : https://euler.ac-versailles.fr/wm3/pi2/crypto/decrypt1.jsp

Correction

https://euler.ac-versailles.fr/wm3/pi2/crypto/decrypt1.jsp

Lettre	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Effectif	0	0	0	24	3	15	12	53	10	0	4	33	0	0	27	6	18	15	2	9	25	34	32	26	4	0
Fréquence en %	0	0	0	6,82	0,85	4,3	3,41	15,06	2,84	0	1,14	9,38	0	0	7,67	1,7	5,11	4,3	0,57	2,56	7,1	9,66	9,1	7,39	1,14	0



La lettre la plus fréquente est le H.

Le H correspondrait donc au E.

Le décalage est donc probablement de 3 lettres vers la droite.

Pour déchiffrer le message on peut donc tenter de décaler en sens inverse de 3 lettres.

Remarque :

Ensuite on a V, puis L, puis W. On a aussi une bonne proportion de D.

V serait A, L serait S et W serait I. En fait pour ces lettres les fréquences sont trop proches pour conclure.

En fait V correspond à S, L V correspond à I et W V correspond à T. D V correspond à A

Lettre du texte	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Véritable lettre				A	B	C	D	**E**	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

On obtient le message suivant :

On a conservé en outre ses lettres à Cicéron, et celles qu'il adressait à ses familiers sur ses affaires domestiques ; quand il avait à leur faire quelque communication secrète, il usait d'un chiffre, c'est-à-dire qu'il brouillait les lettres de telle façon qu'on ne pût reconstituer aucun mot: si l'on veut en découvrir le sens et les déchiffrer, il faut substituer à chaque lettre la troisième qui la suit dans l'alphabet, c'est-à-dire le D à l'A, et ainsi de suite.

(Suétone - Vies des douze Césars, Livre premier, César, LVI)

Fiche 5 « Code de césar » à l'aide de geogebra

Ouvrir un fichier geogebra, préparer la feuille, marquer un point O

Etape 1 : partage du premier disque

- tracer le cercle de centre O et de rayon 5 : ce sera le disque extérieur.
- tracer le cercle de centre O et de rayon 4 (pour l'alphabet).
- Marquer un point A sur le cercle de plus grand rayon (le premier).
- On veut partager le disque en secteurs circulaires identiques, de façon à ce que chacun représente une lettre de l'alphabet.

Quel angle faut-il indiquer sur geogebra pour chacun de ces secteurs ? ……

- Pour tracer l'angle précédent il faut utiliser :  « Angle de mesure donnée ».

Cliquer sur A puis sur le sommet de l'angle O, puis indiquer comme angle l'opération précédente, ceci en mettant des parenthèses autour. L'ordinateur va créer un point A'.

Renouveler l'opération en cliquant sur A' puis sur O ….

On obtient le partage du disque. Les noms des points seront cachés à la fin mais on peut déjà décocher l'affichage des angles pour plus de clarté.

-Tracer les médiatrice de [AA'], puis [A'A'']… (un demi-tour suffit en fait).

- Marquer les points d'intersection des médiatrices avec le cercle de rayon 4.
- Repérer l'instruction texte  : Cliquer sur un des points d'intersection obtenu avec le cercle de rayon 4.

Une fenêtre apparaît, écrire la lettre A dedans puis ok. Pour qu'elle soit plus grande cliquer sur : 

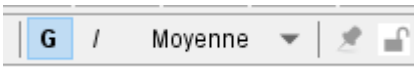
Ne pas s'inquiéter si le nom du point la cache un peu car on le masquera à la fin.

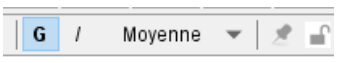
Recommencer avec le point d'intersection suivant en indiquant la lettre B, et ainsi de suite jusqu'à Z.

- Masquer le cercle de rayon 4 ainsi que les médiatrices, les angles (on peut tout faire d'un seul coup avec le bouton droit, puis propriétés, puis décocher afficher objet).
- Tracer tous les rayons du grand cercle (de rayon 5) puis maquer tous les points sauf le point A (le premier sur le cercle) et le point O centre du cercle.

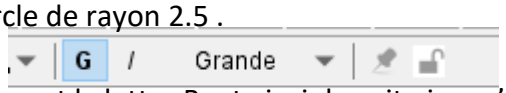
En principe le point A entraîne la rotation de l'alphabet.

Etape 2 : Partage du deuxième disque



- Tracer le cercle de centre O et de rayon 3 (pour l'alphabet).
- Marquer un point B dessus.
- Faire comme pour l'étape 1 le partage avec les mêmes angles, puis les médiatrices et ses points d'intersection avec un cercle cette fois-ci de rayon 2.5.
- Décocher l'affichage des médiatrices.
- Utiliser à nouveau l'instruction « texte » mais plutôt avec : 

Cliquer sur un des points d'intersection obtenu avec le cercle de rayon 2.5 .

Indiquer la lettre A. 

Recommencer avec le point d'intersection suivant en indiquant la lettre B, et ainsi de suite jusqu'à Z.

- Masquer le cercle de plus petit rayon (2.5).
- Tracer tous les rayons du cercle de rayon 3.
- Masquer tous les points sauf B et O.

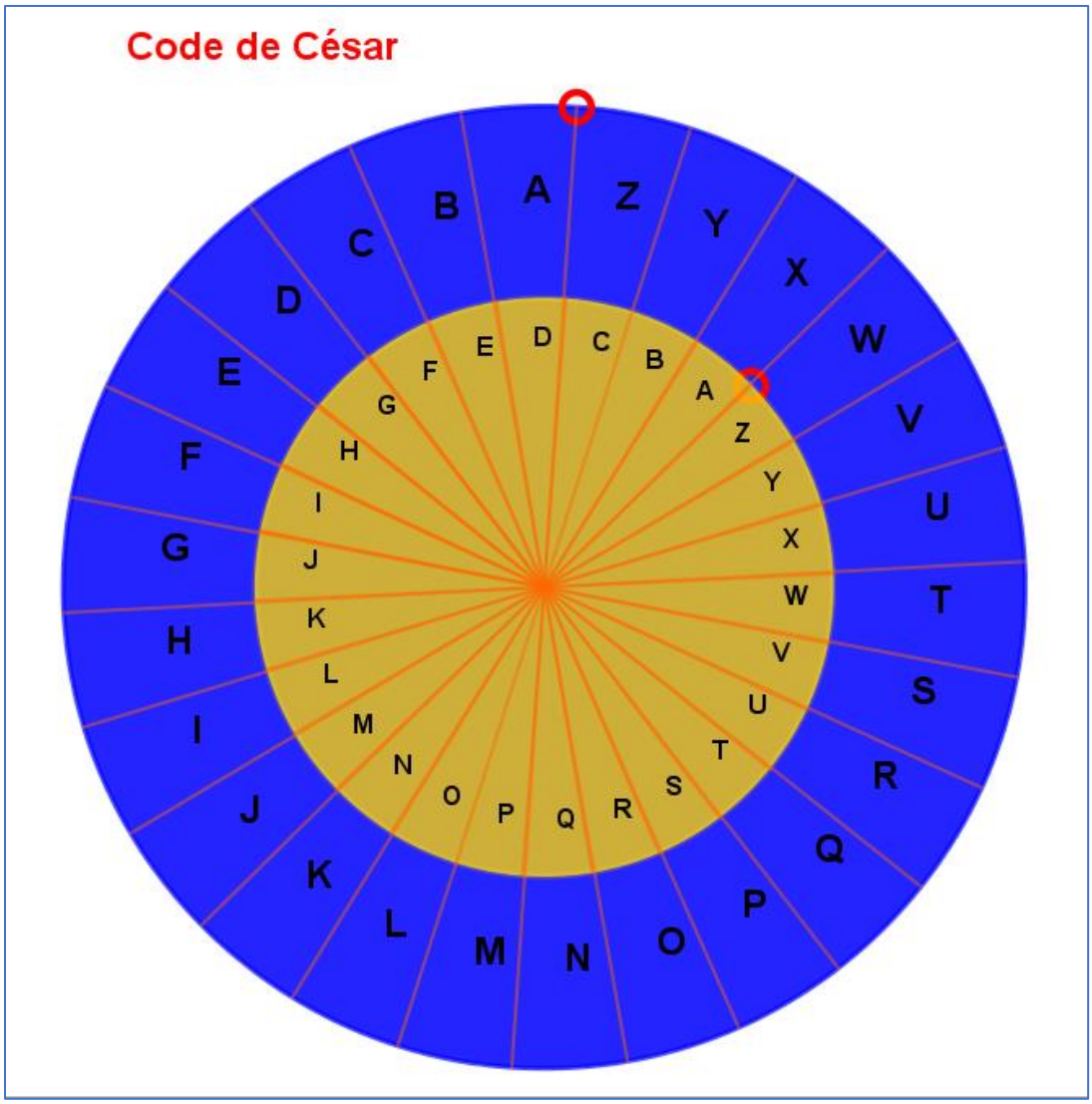
Les points non cachés sont maintenant A, O et B.

Etape 3 : utilisation

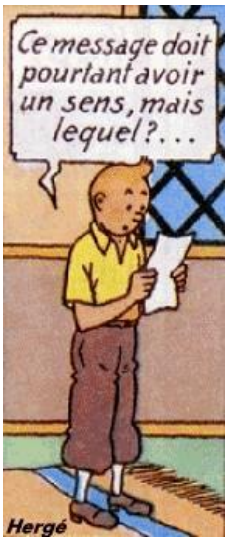
On peut déplacer les points A et B et utiliser de façon très simple le code de césar avec une clé au choix.

Enregistrer le travail sous le nom « code de César ».

Résultat avec geogebra:



Fiche 6 Chiffrage affine



Le code de César est un cas particulier du chiffrement affine.
- Chaque lettre de l'alphabet est d'abord chiffrée : A correspond à 0, B à 1, C à 2….
- Ce nombre est multiplié par un nombre entier a de la liste suivante :

1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25

On y ajoute un nombre entier b $compris$ entre 0 et 25.
Finalement si on appelle x le nombre de départ et y celui que l'on obtient, on a : $y = a \times x + b$
- le nombre obtenu correspond à une lettre de l'alphabet ; s'il est supérieur ou égal à 26, on utilisera le reste de la division euclidienne du résultat par 26.

Ainsi la clé du chiffrement est déterminée par les nombres $a\ et\ b$.
Avec le code de César, c'est en fait la même formule avec : $a = 1\ et\ b = 3$ (en général).
Il y a donc maintenant bien plus de clés possibles.

Exemple 1 : avec $a = 3\ et\ b = 2$ $y = 3 \times x + 2$

Compléter le tableau suivant puis déchiffrer le message suivant : « IOJC LONAOPH ISMVJAYKO »

Lettre du texte	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Lettre x chiffrée	0	1	2	3	4	5	6	7	**8**																	
Calcul y	$0 \times 3 + 2 = 0 + 2 = 2$	$1 \times 3 + 2 = 3 + 2 = 5$																								
Véritable lettre	C	F																								

Exemple 2 : quel serait le problème avec les nombres suivants : $a = 2\ et\ b = 3$?

$y = 2 \times x + 3$

Compléter le tableau suivant :

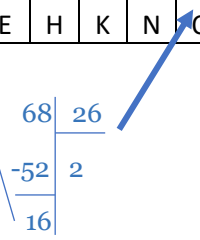
Lettre du texte	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Lettre x chiffrée	0	1	2	3	4	5	6	7	8																	
Calcul y	3	5																								
Véritable lettre	D	F																								

Conclusion : attention à ne pas choisir a et b au hasard !

Correction

Exemple 1

Lettre du texte	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Lettre chiffrée	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Calcul	2	5	8	11	14	17	20	23	**26**	29	32	35	38	41	44	47	50	53	56	59	62	65	68	71	74	77
Véritable lettre	C	F	I	L	O	R	U	X	**A**	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z



IOJC LONAOPH ISMVJAYKO signifie : cela devient compliqué !

En fait y est le reste de la division euclidienne de 3x+2 par 26

68 et 16 ont le même reste dans la division euclidienne par 26.

Exemple 2 : quel serait le problème avec les nombres suivants : $a = 2$ *et* $b = 3$

$$y = 2 \times x + 3$$

Compléter le tableau suivant :

Lettre du texte	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Lettre x chiffrée	0	1	2	3	4	5	6	7	8																	
Calcul y	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31											
Véritable lettre	D	F	H	J	L	N	P	R	T	V	X	Z	B	D	F											

	0 A		0 A	
	1 B		1 B	
	2 C		2 C	
	3 D		3 D	
	4 E		4 E	
	5 F		5 F	
	6 G		6 G	
	7 H		7 H	
	8 I		8 I	
	9 J		9 J	
	10 K		10 K	
	11 L		11 L	
	12 M		12 M	
	13 N		13 N	
	14 O		14 O	
	15 P		15 P	
	16 Q		16 Q	
	17 R		17 R	
	18 S		18 S	
	19 T		19 T	
	20 U		20 U	
	21 V		21 V	
	22 W		22 W	
	23 X		23 X	
	24 Y		24 Y	
	25 Z		25 Z	

Fiche 7 Carré de Vigenère

Blaise de Vigenère (1523-1596) était un diplomate français. Le système suivant est une amélioration du chiffre de César. Dans un code César, le chiffrement est **monoalphabétique** : à l'alphabet en clair correspond un seul alphabet chiffré, de sorte qu'à chaque lettre corresponde toujours le même caractère chiffré (par exemple dans le code César avec la clé 3, la lettre A correspond toujours à la lettre D).
Dans un chiffrement **polyalphabétique**, à une lettre donnée d'un message, il peut correspondre autant de lettres que d'alphabets chiffrés employés. Pour coder le texte, on passe d'un alphabet chiffré à l'autre à chaque fois que l'on passe d'une lettre de l'alphabet en clair à une autre. Le premier et le plus célèbre des chiffrements polyalphabétiques est le « carré de Vigenère ». Ainsi la même lettre sera chiffrée de différentes manières, ce qui rend **inutilisable l'analyse des fréquences.**

Question 1:
- Compléter ce carré (lignes C, M et U)
- On choisit en général ensuite une clé, un mot, par exemple : « sixieme ».
- Utiliser ceci pour crypter le message 1 : « Le coupable est »
- Décrypter le message 2 : SZPMRQPMXFV

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**
C																										
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**
M																										
N	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
O	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**
P	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**
Q	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**
R	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**
S	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**
T	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**
U																										
V	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**
W	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**
X	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**
Y	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**
Z	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**

Message 1 clair	L	E	C	O	U	P	A	B	L	E	E	S	T
Clé	**S**	**I**	**X**	**I**	**E**	**M**	**E**	**S**	**I**	**X**	**I**	**E**	**M**
Message 1 crypté	D	M											

Message 2 : SZPMRQPMXFV

Message 2 crypté	S	Z	P	M	R	Q	P	M	X	F	V		
Clé	S	I	X	I	E	M	E	S	I	X	I		
Message décrypté	A	R											

Correction

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**
N	n	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
O	o	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**
P	p	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**
Q	q	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**
R	r	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**
S	s	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**
T	t	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**
U	u	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**
V	v	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**
W	w	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**
X	x	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**
Y	y	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**
Z	z	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**

Message 1 : Le coupable est :

Message 1 non codé	**L**	E	C	O	U	P	A	B	L	E	E	S	T
Clé (mot secret)	**S**	**I**	**X**	**I**	**E**	**M**	**E**	**S**	**I**	**X**	**I**	**E**	**M**
Message 1 codé	**D**	M	Z	W	Y	B	E	T	T	B	M	W	F

On regarde la ligne S et la colonne L, et on repère la lettre intersection des deux : c'est D.

Message 2 : SZPMRQPMXFV **Raisonner à l'envers pour faire déchiffrer un message « Arsène Lupin »**

Message 2 codé	**S**	Z	P	M	R	Q	P	M	X	F	V		
Clé	**S**	I	X	I	E	M	E	S	I	X	I		
Message déchiffré	**A**	R	S	E	N	E	L	U	P	I	N		

On regarde la ligne I, dedans on repère la lettre Z, et on regarde la colonne correspondante : c'est R.

https://euler.ac-versailles.fr/wm3/pi2/vigenere/vigenere1.jsp

Fiche 8 XIXème siècle : Le code Morse

Le XIXème siècle a donné un nouvel intérêt aux codes : l'invention du télégraphe a révolutionné les communications. Il fonctionnait par impulsions électriques ; il a donc fallu traduire le contenu des messages des gens en un langage « compréhensible » par la machine, et inversement. Ce fut un système de traits et de points, conçu par un peintre et physicien américain : **Samuel Morse**, qui fut adopté. La première transmission a eu lieu en 1844 (1re ligne entre Washington et Baltimore)

Chaque point représentait une unité de temps d'une durée approximative de 1/25 de seconde et chaque trait 3 unités. Pour transme ttre des télégrammes traditionnels, un opérateur était nécessaire pour taper la version codée du message et un autre pour la lire.

A	·–	N	–·	0	–––––
B	–···	O	–––	1	·––––
C	–·–·	P	·––·	2	··–––
D	–··	Q	––·–	3	···––
E	·	R	·–·	4	····–
F	··–·	S	···	5	·····
G	––·	T	–	6	–····
H	····	U	··–	7	––···
I	··	V	···–	8	–––··
J	·–––	W	·––	9	––––·
K	–·–	X	–··–	.	·–·–·–
L	·–··	Y	–·––	,	––··––
M	––	Z	––··	?	··––··

Samuel Morse (1791-1872)

Question : - Traduire SOS en langage morse :
- sous scratch…

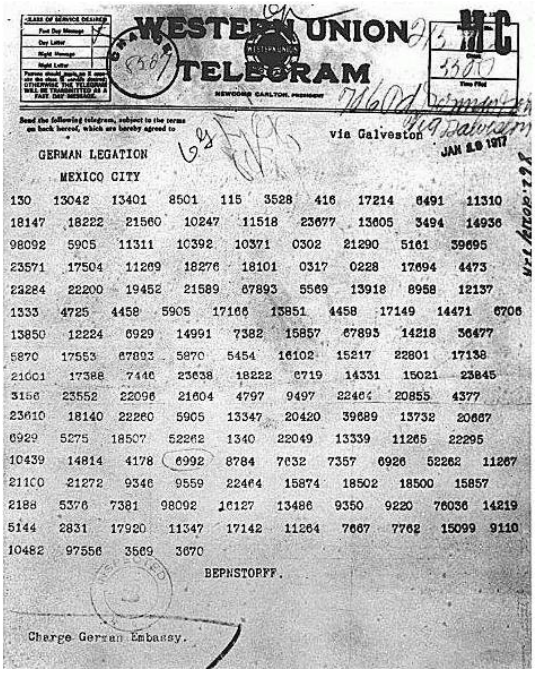
Remarque : utilisation de nos jours : https://www.jpl.nasa.gov/news/news.php?release=2012-266

« NASA's Curiosity rover took its first test stroll Wednesday Aug. 22, 2012, and beamed back pictures of its accomplishment in the form of track marks in the Martian soil…The pattern is Morse code for JPL, the abbreviation for NASA's Jet Propulsion Laboratory in Pasadena, Calif., where the rover was designed and built, and the mission is managed…This driving tool, called visual odometry, allows the rover to use images of landscape features to determine if it has traveled as far as predicted, or if its wheels have slipped…The Morse code imprinted on all six wheels will be particularly handy when the terrain is barren. »

Traduction : Le rover Curiosity de la NASA a effectué sa première promenade d'essai le mercredi 22 août 2012 et a retransmis des images de sa réalisation sous forme de traces sur le sol martien…Le modèle correspond au code Morse pour JPL, abréviation de Jet Propulsion Laboratory de la NASA à Pasadena, en Californie, où le rover a été conçu et construit et où la mission est gérée…Cet outil de conduite, appelé odométrie visuelle, permet au mobile d'utiliser des images de caractéristiques du paysage pour déterminer s'il a voyagé aussi loin que prévu ou si ses roues ont glissé…Le code Morse imprimé sur les six roues sera particulièrement utile lorsque le terrain est dénudé.

Fiche 9 Au XXème siècle : des tournants dans les deux guerres mondiales

16 janvier 1917 *Télégramme de Zimmermann*



WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 59695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

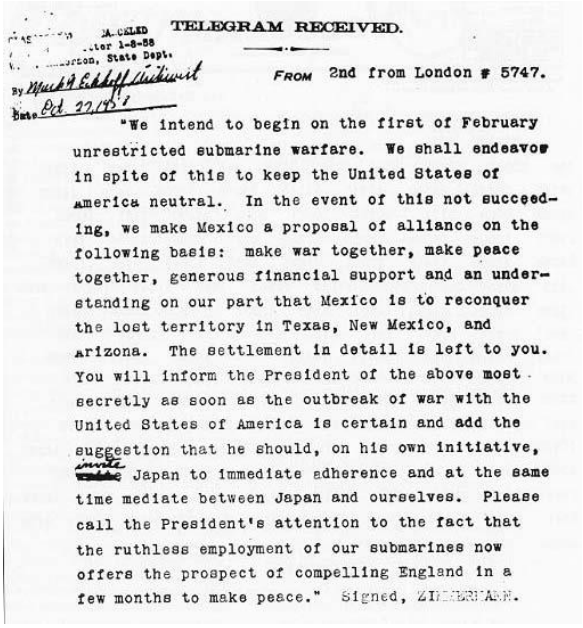
BEPNSTORFF.

Charge German Embassy.

En janvier 1917, le Commandement allemand essayait de persuader le Kaiser qu'il était temps de déclencher une guerre sous-marine totale pour couper les approvisionnements de la Grande-Bretagne et ainsi l'affamer. Le risque était qu'une guerre sous-marine totale, avec pour conséquence inévitable la destruction de bateaux civils américains, inciterait à coup sûr les États-Unis à déclarer la guerre à l'Allemagne. Dans cette perspective, l'Allemagne se devait d'obtenir une capitulation rapide des Alliés avant que l'Amérique puisse mobiliser ses troupes et peser de tout son poids sur le champ de bataille européen. Le Kaiser fut convaincu qu'une victoire rapide était possible et signa un ordre de passer à la guerre sous-marine sans restriction, à dater de premier février 1917. **Arthur Zimmermann** ministre allemand, avait un plan pour réduire ou retarder l'engagement américain, voire l'empêcher : proposer une alliance au Mexique et encourager son président à envahir les États-Unis. L'Allemagne soutiendrait le Mexique financièrement et militairement, et propose en cas de victoire, l'annexion du Sud des États-Unis.

Le 16 janvier, Zimmermann formula sa proposition dans un télégramme codé à l'ambassadeur d'Allemagne à Washington, à retransmettre à l'ambassadeur d'Allemagne à Mexico, puis au président du Mexique.

Le télégramme codé fut intercepté par les Britanniques et immédiatement transmis au **bureau 40**. Ce fut le révérend Montgomery qui fut chargé de le déchiffrer, avec l'aide de Nigel de Grey. Ils virent immédiatement qu'ils avaient affaire à une forme de cryptage utilisée uniquement pour des communications diplomatiques au plus haut niveau. Le décryptement était loin d'être aisé, mais ils pouvaient s'appuyer sur des analyses précédentes de télégrammes cryptés de la même façon. Le télégramme fut décrypté le 22 février 1917.



TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Traduction Nous avons l'intention de déclencher le premier février une guerre sous-marine totale. Malgré cela, nous tenterons de maintenir les États-Unis dans la neutralité. Si nous n'y parvenons pas, nous proposerons au Mexique une alliance sur les bases suivantes: faire la guerre ensemble, faire la paix ensemble, large soutien financier et accord de notre part pour la reconquête par le Mexique des territoires perdus du Texas, du Nouveau Mexique et de l'Arizona. Le règlement des détails est laissé à votre initiative.
Dès que l'ouverture des hostilités avec les États-Unis sera certaine, vous informerez très secrètement le président [du Mexique] de ce qui précède et vous lui suggérerez qu'il devrait, de sa propre initiative, solliciter la participation immédiate du Japon et proposer simultanément sa médiation entre le Japon et nous. Prière d'attirer l'attention du président sur le fait que l'emploi sans restriction de nos sous-marins offre maintenant la possibilité d'obliger en peu de mois l'Angleterre à faire la paix.

Zimmerman

Le télégramme décrypté fut diffusé dans la presse et la nation américaine se trouva enfin confrontée aux intentions véritables de l'Allemagne. Ce télégramme incita aussi le président américain Wilson, qui avait déclaré que ce serait «un crime contre la civilisation» de laisser entraîner son pays dans la guerre, à changer d'avis et à recommander au Congrès d'entrer en guerre contre l'Allemagne, ce qui fut fait. Ainsi, le décryptement par le bureau 40 d'un message ennemi contribua à l'entrée en guerre des États-Unis dans la Première Guerre Mondiale, assurant ainsi la victoire des Alliés.

https://www.francetvinfo.fr/replay-radio/france-info-y-etait/2-avril-1917-le-president-des-etats-unis-demande-la-guerre_1752887.html

Fiche 9 Au XXème siècle (suite)

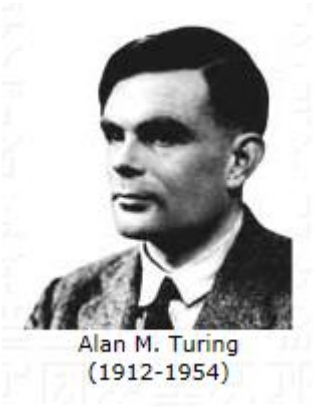
Machine Enigma :

En 1923, l'ingénieur allemand Arthur Scherbius breveta une machine conçue pour faciliter les communications sécurisées.

Son nom : Enigma, et plusieurs modèles…

En raison de sa facilité d'utilisation et la complexité du chiffrement, Enigma fut choisie par le gouvernement allemand comme base de codage d'une bonne partie de son trafic de communications militaires pendant la seconde guerre mondiale.

Le décryptage d'Enigma devint donc une priorité des gouvernements qui affrontèrent l'Allemagne nazie.


Alan M. Turing
(1912-1954)

Au début des années 1940, une équipe de 7000 personnes réussit à percer le secret des messages allemands chiffrés par Enigma. Cette armée, rassemblée en grand secret à Bletchley Park, au nord-ouest de Londres, réunit des mathématiciens, des érudits en tout genre... dont un génie, Alan Turing. Cela permet aux Alliés de tout savoir sur les projets des Allemands et sur les mouvements de leurs troupes.

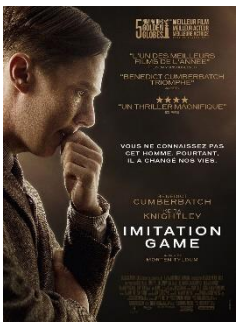
Parmi ces actions, en 1942, un amiral américain, Chester Nimitz, devait faire face à l'armée japonaise, à l'amiral Yamamoto. Celui-ci avait décidé d'attaquer par surprise une base située au milieu du Pacifique, Midway. Le bombardement commençait quand des bombardiers américains se sont lancés à l'assaut, et que la flotte américaine était prête au combat : 4 porte-avions sont coulés côté japonais, 1 seul côté américain. En fait Nimitz lisait dans le jeu de son ennemi. Ses cryptanalystes avaient cassé le code japonais, avaient anticipé l'attaque de Midway et piégé Yamamoto.

Toutes les informations collectées n'étaient pas utilisées de peur que les Allemands se rendent compte que leur machine Enigma n'était plus du tout sûre et qu'ils compliquent encore leur système. Beaucoup de vies alliées, notamment celles des marins des convois qui traversaient l'Atlantique, ont ainsi été sacrifiées.

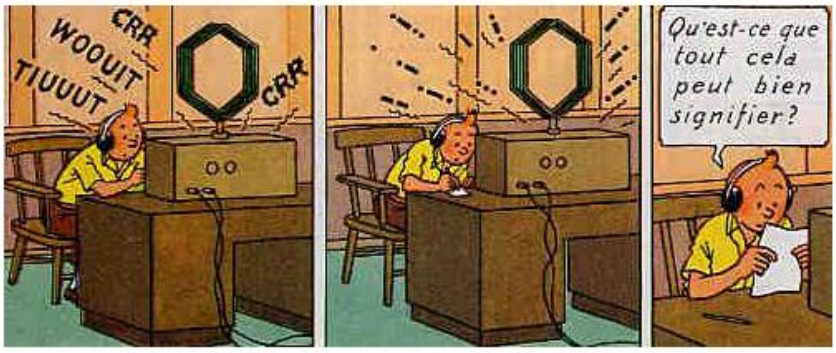
Fonctionnement :

http://www.youtube.com/watch?NR=1&v=2b6xSuMsoY8&feature=endscreen

https://www.francetvinfo.fr/replay-radio/ils-ont-fait-le-web/alan-turing_1787347.html



Fiche 10 Aujourd'hui et demain



Depuis la Seconde Guerre Mondiale, les besoins cryptographiques ont explosé. Les applications civiles du chiffrement (banques, télécommunications, informatique, cartes bleues...) deviennent un moteur fondamental de progrès. La généralisation de l'outil informatique permet d'exploiter des algorithmes bien plus complexes, mais dans le même temps les attaques peuvent être automatisées.

En effet le problème le plus important est celui de l'échange des clés entre l'émetteur et le destinataire du message, la clé utilisée étant la même pour le chiffrement que pour le déchiffrement (clé « symétrique »).

La méthode de cryptographie RSA a été inventée en 1977 par trois américains : Ron **R**ivest, Adi **S**hamir et Len **A**dleman, à la suite de la découverte de la cryptographie à clé publique par Diffie, Hellman et Merkle.

Cette fois-ci la clé est « asymétrique » : la clé de chiffrement (clé publique) serait différente de la clé de déchiffrement (clé privée)

La fiabilité des clés du système RSA nécessite l'utilisation de nombres premiers très grands :

Dans l'exemple de la page qui va suivre, n et T sont publiques, un espion peut les connaître. Mais pour M, cette clé est privée. Elle dépend de n et de T, au final il faut connaître p et q.

L'espion devrait donc décomposer n comme produit de deux nombres premiers. Or si n est très grand (200 chiffres par exemple). C'est très difficile….

Un exemple très simplifié a été donné aux élèves.

L'avenir : il devrait être quantique…

Fiche récapitulative : à faire par chaque élève

1) Coder le message suivant avec chacun des moyens étudiés : « Arsene Lupin est le coupable »

Remarque: pour la stéganographie, on peut prendre le message en photo et le cacher sous geogebra.

2) Essayer de décoder le message du 1) et repérer ce qu'il faut indiquer au destinataire : clé, instrument, explication, fichier, disques….

Fabriquer les outils nécessaires :

- pour la scytale, on peut choisir un stylo, mais aussi utiliser un rouleau type « Sopalin » et le décorer.
- pour Polybe, recopier proprement le carré sur une feuille et le coller sur un papier type « canson » ou cartonné, faire une belle présentation ; ceux qui peuvent plastifier, n'hésitez pas.
- pour le code César, c'est en principe déjà fait, le terminer si nécessaire
- pour le chiffrage affine, utiliser la fiche distribuée pour en refaire un, identique ou non, bien écrit, collé sur une feuille type « canson » ou cartonnée, éventuellement plastifiée, avec éventuellement un laçage pour la réponse (sinon des traits au feutre)
- Pour le code Vigenère : soit écrire à la main toutes les lettres (ce sera plus joli) puis coller sur papier canson, soit utiliser directement la photocopie et la coller sur du papier épais ; puis plastifier pour ceux qui peuvent, et sinon, l'insérer dans une pochette plastique ; prévoir comme accessoire un feutre « véléda » pour écrire dessus.

3) Ecrire quelques phrases explicatives pour une personne voulant décoder le message.

4) Ecrire quelques phrases indiquant ce que nous avons fait en mathématiques : pour concevoir la partie mathématique du jeu, et pour jouer.

Code	Résultat obtenu (écrire le résultat ou la méthode)	Outil à fournir
Stéganographie		
Scytale		
Polybe		
César		
Chiffrage affine		
Vigenère		
Code Morse		

Fiche récapitulative- correction

Coder le message suivant avec chacun des moyens étudiés : « Arsene Lupin est le coupable »

Code	Résultat obtenu (écrire le résultat ou la méthode)	Outil à fournir
Stéganographie		Fichier et angles
Scytale		Donner la scytale et l'explication
Polybe	11 43 44 15 34 15 32 51 41 24 34 15 44 45 32 15 13 35 51 41 11 12 32 15	Donner le carré et l'explication
César avec A transformé en C	CTUGPG NWRKP GUV NG EQWRCDNG	Disque et clé : dire de décaler de 2 lettres
Chiffrage affine Avec y=5x+1	BINVOV EXYPO VNS EV LTXYBGEV	Laçage fait ou non
Vigenère Avec le mot secret : sixieme	SZPMRQPMXFVIEXDMZWYBETTB	Le carré avec le feutre veleda, l'explication et le mot secret.
Code Morse	.- .-. ... . -. ./ .-.. ..- .--. .. -./ . ... -/ .-.. ./ -.-. --- ..- .--. .- - .../ .-.. .	Donner le code ; bien séparer les mots et surtout les lettres (éventuellement une couleur différente pour chaque lettre).

Exemple 1 de phrases à coder

Tous les élèves ont crypté cette phrase: « Il n'y a aucun indice ici. »

Code	Résultat obtenu (écrire le résultat ou la méthode)
Stéganographie	
Scytale	
Polybe	**24 32 34 54 11 11 51 13 51 34 24 34 14 24 13 15 24 13 24**
César avec A transformé en C	**KN PA C CWEWP KPFKEG KEK**
César avec A transformé en D	**LO Q B D DXFXQ LQGLFH LFL**
César avec A transformé en R (+17)	ZC E P R RLTLE ZEUZTV ZTZ
Chiffrage affine Avec y=3x+2	**AJ PW C CKIKP APLAIO AIA**
Chiffrage affine Avec y=5x+1	**ICFCNEFWJVVNUAGRMNC.**
Vigenère Avec le mot secret : sixieme	**AT KG E MYUCK QRPMUM FKM**
Code Morse	../ .-.. // -./ -.--// .-// .- /..-/ -.-./ ..-/ -. // .. / -./ -../ ../ -.-. /. // ../ -.-. /..

Exemple 2 de phrases à coder

Chaque élève a codé également une des phrases d'une des énigmes.

Phrases à coder

Par exemple, pour l'énigme 2, un élève a pris en charge la phrase « C'est le comte de Gesvres qui a tué Jean Daval.»

Code	Résultat obtenu (écrire le résultat ou la méthode)
Stéganographie	
Scytale	
Polybe	13 15 44 45 32 15 13 35 33 45 15 14 15 22 15 44 52 43 15 44 42 51 24 11 45 51 15 25 15 11 34 14 11 52 11 32
César avec A transformé en C	G IWX PI GSQXI HI KIWZVIW UYM E XYI NIER HEZEP
Chiffrage affine Avec y=5x+1	L VNS EV LTJSV QV FVNCIVN DXP B SXV UVBO QBCBE
Vigenère Avec le mot secret : ArseneLupin	C VKX YI NIBBR DV YIFZCYH YHI R LYR NPUC LNVRD.
Code Morse	-.-./ ./ .../ - // .-.. /. // -.-./ ---/ --/ - /. // -../ . // --. /./ .../ ...- /.-./ ./ ...// --.-/..- /.. // .- // - /..-/ . // .--- /./ .-/ -. // -../ .-/ ...- /.- /.-..

Pour les vérifications des phrases une par une, les ressources sur Euler furent plus qu'utiles…